IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of:	)	Confirmation No.: 1004
	)	
Rae K. Burns, et al.	)	Examiner: Leslie Wong
	)	
Serial No.: 10/006,543	)	Group Art Unit No.: 2164
	)	
Filed on: November 30, 2001	)	
	)	

For: TECHNIQUES FOR ADDING MULTIPLE SECURITY POLICIES TO A DATABASE SYSTEM

Via EFS-Web
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

This Appeal Brief is submitted (a) in support of the Notice of Appeal, which was filed on April 9, 2008, and (b) in response to the Notice of Panel Decision from Pre-Appeal Brief Review, which was mailed on May 16, 2008.

I. REAL PARTY IN INTEREST

Oracle International Corporation is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals or interferences.

III. STATUS OF CLAIMS

Claims 1-40 are pending in this application and were finally rejected in the Final Office Action that was mailed on October 29, 2007. No claims were added or cancelled.

Claims 1-40 are the subject of this appeal.

IV. STATUS OF AMENDMENTS

An amendment to Claims 6, 13, and 21-40 was filed in the reply to the Final Office Action, which reply was filed on December 13, 2008. As indicated in the Advisory Action mailed on March 24, 2008, those amendments were not entered. No amendments were filed after the reply to the Final Office Action.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present application contains independent Claims 1, 6, 21, and 26.

A. CLAIMS 1 AND 21

Claim 1 is generally directed to a method for managing access to data in a database subject to a plurality of label-based security policies (FIGs. 1A and 3). Within a database management system, a request for performing an operation set of one or more operations on data in a table of the database is received. (Specification, paragraph 79 and FIG. 3). It is determined which policies, of the plurality of label-based policies, apply to the table based on a policy set of one or more policies associated with the table. (Specification, paragraph 80 and FIG. 3). For each operation in the operation set, it is determine whether to perform the operation on a row of the table based on a set of labels associated with the row, the set of labels corresponding to the policy set. (Specification, paragraphs 81-83).

Independent Claim 21 is a computer-readable medium counterpart of method Claim 1, and includes limitations analogous to the limitations of Claim 1. Thus, elements of Claim 21 are disclosed in at least the same sections of the Specification and Drawings as those cited above in connection with Claim 1. In addition, other elements of Claim 21 are supported by the hardware and computer-readable media description provided on paragraphs 92-101 of the Specification.

B. CLAIMS 6 AND 26

Claim 6 is generally directed to a method for managing access to data in a database based on a database policy set of one or more label-based security policies. One or more packages of routines are registered with a database management system. (Specification,

paragraph 57 and FIGs. 1B and 2). Each package of said one or more packages implements a security model that supports a model set of one or more policies of the database policy set. (Specification, paragraphs 16, 49, and 50 and FIG. 1B). Each package also includes an access mediation routine. (Specification, paragraphs 50-51 and FIG. 1B). A first policy of a first model set in a first package is associated with a first table within the database system. (Specification, paragraphs 16, 43, 44, 51, and 67). The access mediation routine in the first package is invoked to determine, based on the first policy, whether to allow an operation on data in the first table. (Specification, paragraphs 56 and 68 and FIGs. 2-3).

Independent Claim 26 is a computer-readable medium counterpart of method Claim 6, and includes limitations analogous to the limitations of Claim 6. Thus, elements of Claim 26 are disclosed in at least the same sections of the Specification and Drawings as those cited above in connection with Claim 6. In addition, other elements of Claim 26 are supported by the hardware and computer-readable media description provided on paragraphs 92-101 of the Specification.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-5 and 21-25 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent Publication No. 2002/0143735 to Ayi et al. ("*Ayi*") in view of U.S. Patent No. 5,787,428 issued to Hart ("*Hart*").

Claims 6-20 and 26-40 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent No. 5,859,966 issued to Hayman et al. ("*Hayman*") in view of *Ayi*.

VII. ARGUMENTS

It is also respectfully submitted that the examiner has erred in rejecting Claims 1-40 under 35 U.S.C. § 103(a).

A. CLAIMS 1-5 AND 21-25

Claims 1-5 and 21-25 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Ayi* in view of *Hart*.

37 C.F.R. § 1.131 states, in part:

> (a) When any claim of an application…is rejected, the inventor…may submit an appropriate oath or declaration to establish invention of the subject matter of the rejected claim prior to the effective date of the reference.
>
> (b) The showing of facts shall be such, in character and weight, as to establish reduction to practice prior to the effective date of the reference…. Original exhibits of drawings or records, or photocopies thereof, must accompany and form part of the affidavit or declaration or their absence must be satisfactorily explained.

It is the Examiner's position that the evidence submitted under 37 C.F.R. § 1.131 is insufficient to establish an actual reduction to practice of the invention, according to Claims 1-5 and 21-25, prior to the effective date of *Ayi* (page 2). The Examiner contends that the subject declaration (a) amounts to a general allegation and (b) lacks a statement of the facts demonstrating the correctness of the declaration, by the inventors, that the invention was reduced to practice prior to the effective date of *Ayi* (page 2). It is respectfully submitted that this is incorrect.

It is respectfully noted that the Examiner has failed to address, in the Final Office Action (mailed October 29, 2007) and the Advisory Action (mailed March 24, 2008), any of the arguments presented in the response mailed on August 14, 2007, some of which are repeated below.

On page 3 of the Final Office Action, the Examiner refers to a statement from a prior response, which states:

> Obviously, **test script files and test script log files do not show the actual code that performs recited steps**. Therefore, for example, it is difficult to show the step of "determining which policies…" and the step of "determining whether to perform the operation." (emphasis added)

In response to this statement, the Examiner contends that "without correlating the limitations of at least the independent claims to Applicant's Exhibits, the Applicant has failed to show possession of the claimed invention." Representatives of the Applicants respectfully request the Examiner to point out in the CFR and/or MPEP where it is required that limitations of the claims must be correlated to exhibits. In fact, 37 C.F.R. § 1.131 provides the standard for the sufficiency of a showing of a reduction to practice:

> **The showing of facts shall be such, in character and weight, as to establish reduction to practice prior to the effective date of the reference**.... Original exhibits of drawings or records, or photocopies thereof, must accompany and form part of the affidavit or declaration or their absence must be satisfactorily explained. (emphasis added)

As is clear, an Examiner is not required to find a correlation between (a) all the limitations in a claim and (b) exhibits in order to find the sufficiency of a declaration under 37 C.F.R. § 1.131. Rather, the standard is that the "showing of facts shall be such, in character and weight, as to establish reduction to practice prior to the effective date of the reference."

Also on page 3 of the Final Office Action, the Examiner quotes MPEP § 715.02, which states: "If the **affidavit contains** facts showing a completion of the invention commensurate with the extent of the invention as claimed is shown in the reference or activity, the affidavit or declaration is sufficient" (emphasis in the Final Office Action). **This section of the MPEP actually supports the Applicants' position**. The present declaration satisfies the criteria specified in MPEP § 715.02, i.e., the declaration contains facts showing a completion of the

invention commensurate with the extent of the invention as claimed. For example, the declaration states:

> 3. We conceived and **reduced to practice *an implementation*** **of claims 1 – 5 and 21 - 25** before the effective filing date of Ayi.
>
> 4. We participated on a team that developed the implementation of **claims 1 – 5 and 21 – 25** that is incorporated into an Oracle™ database server product. After the design phase of the development, **successful tests were run to show that the implementation worked according to claims 1 – 5 and 21 - 25**. These tests, which were conducted using standard internal test processes and procedures, were completed before the effective filing date of Ayi and were carried out in this country.

(emphasis added)

Therefore, the declaration is **sufficient**.

On page 4 of the Final Office Action, the Examiner provides patent office policy for actual reductions to practice under 37 CFR § 1.131, which office policy apparently states:

> a. Testing is required unless operativeness of invention is readily apparent.
> b. Testing, if required, must be under actual working conditions or realistic simulation of working conditions.
> c. Test results must be repeatable.

In support of this policy, the Final Office Action cites MPEP § 2138.05. However, MPEP § 2138.05 pertains to interference practice and **37 CFR 1.131 does not apply in interference proceedings** (see MPEP 2138.01(III)). Neither the CFR nor the MPEP require testing in a Rule 131 declaration. Nevertheless, the inventors stated in the declaration that "**successful tests were run to show that the implementation worked** according to claims 1 – 5 and 21 – 25" (¶ 4; emphasis added). Furthermore, software tests are clearly repeatable. If ¶ 4 of the declaration was considered by the Examiner, then it is appears from the Examiner's appeal for testing of the invention that the Examiner might want to personally witness tests being run. However, there is no such requirement. Instead, MPEP § 715.07(I) requires examiners to "consider all of the *evidence* presented in its entirety, **including the…declarations**" (emphasis added). Thus,

because the declaration is also evidence of a reduction to practice of the invention, the declaration must be considered.

Finally, on page 4 of the Final Office Action, the Examiner states that "the examiner cannot determine whether or not the reduced to practice invention is commensurate with the claims **without the nexus between the claim and the Exhibit. As a result, the Examiner has no basis to approve the affidavit**" (page 4; emphasis in the Final Office Action). It is respectfully submitted that the Examiner has ample basis to approve the declaration.

First, the statements by the inventors in the subject declaration are **not** hollow assertions. Rather, they are specific statements of fact. (Again see MPEP § 715.07(I) which states that evidence includes the declaration.) As such, the statements are considered evidence, each of which cannot be ignored.

Second, the courts have stated that "the PTO is required to accept Rule 131 Affidavits at **face value**, and **without investigation**" (see, e.g., Herman v. Williams Brooks Shoe Co., 39 USPQ2d 1773, 1777 (S.D. N.Y. 1996); see also Chisum on Patents § 3.08[1][a] (2005); emphasis added). Based on the specific evidence provided in the declaration, the inventors have satisfied their burden to prove that a working implementation of the invention according to Claims 1-5 and 21-25 existed prior to the effective filing date of *Ayi*.

Third, MPEP § 715.07 states, "**An accompanying exhibit need not support all claimed limitations**, provided that any missing limitation is supported by the declaration itself." Indeed, exhibits are not even required by 37 CFR § 1.131 or the MPEP. Exhibits A-D are either test script files or test script log files that show results of running the corresponding test script. The exhibits do not provide the actual code. However, neither the CFR nor the MPEP **require code to be submitted** in an exhibit, nor do the CFR and MPEP require a declaration to state word-for-word each claim limitation. To require a declaration to state

word-for-word each claim limitation would be mere form over substance since Applicants may simply recite each claim limitation and state that such claim limitation was implemented before a certain date. Nevertheless, the **inventors have done effectively as much when referring** (1) specifically to Claims 1-5 and 21-25 in ¶ 3, 4, and 9 of the declaration and (2) implicitly in the remaining statements. Therefore, it is odd that the Final Office Action would state that "the examiner cannot determine whether or not the reduced to practice invention is commensurate with the claims." Contrary to this assertion in the Final Office Action, the Applicants have given "a clear explanation of the exhibits [in the declaration] pointing out exactly what facts are established and relied on by applicant." MPEP § 715.07.

As stated above, the Patent Office is required to accept Rule 131 declarations at face value, without investigation. Based on the foregoing, it is respectfully submitted that the declaration and the accompanying exhibits are sufficient to prove a reduction to practice of the invention.

B. CLAIMS 3, 5-8, 11, 15, 17-20, AND 23

Claims 6-20 and 26-40 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Hayman* in view of *Ayi*.

1. Claims 6 and 26

Claims 6 and 26 recite:

> **registering**, with a database management system, **one or more packages** of routines, wherein each package of said one or more packages implements a security model **that supports** a model set of **one or more policies** of the database policy set **and said each package includes an access mediation routine**;
> **associating a first policy** of a first model set in a first package **with a first table** within the database system; and
> **invoking the access mediation routine in the first package for determining whether to allow operation on data in the first table based on the first policy**. (emphasis added)

Claims 6 and 26 require that: (1) a package is registered with a database management system; (2) the package implements a security model that supports a policy; (3) the package includes an access mediation routine; (4) the policy is associated with a table; and (5) the access mediation routine is invoked to determine, based on the policy, whether an operation on data in the table is allowed.

Fundamentally, Claims 6 and 26 require that after **a policy of a package is associated with a table, an access mediation routine <u>of that same package</u> is invoked to determine whether an operation is allowed on data of that table**. This feature is not taught or suggested by *Hayman* or *Ayi*, either individually or in combination. On page 9 of the Final Office Action, the Examiner cites *Hayman* for disclosing all features of Claims 6 and 26 except for the recited first table (page 9). *Ayi* is only cited to show that labels are applied to tables.

On page 8 of the Final Office Action, the Examiner alleges that the "applicant admits that registering one or more packages of routines are well known in the art" on page 17 of the Specification. This is plainly incorrect. The italicized sentence below is taken completely out of context. The applicable language from the Specification states:

> In step 212 a first security model package is registered with the security manager 132 of the database server 130. In some embodiments, the database security administrator designs and develops the security model package. In some embodiments the security model package is provided by the developer of the security manager 132, or is provided by a third party vendor, so that a database administrator does not have to develop her own package. For example, a security model package 110 that supports a compartmented security model is provided by the developer of the security manager, and the database security administrator registers the package 110 with the database server 130. *Any manner known in the art for registering the package at the time the package is registered can be used.* **For example, the database security administrator types in a name of the file containing the package in a dialog box of a graphical user interface for the security manager 132** of the database server 130 (page 17, paragraph 57) (emphasis added).

Clearly, what is meant by "any manner known in the art for registering the package at the time the package is registered can be used" is that the manner in which a package is **identified** (e.g., via dialog box of a GUI or DOS command) for being registered is not important. However, nothing in the Specification implies or suggests that previous database systems actually register one or more packages of routines as claimed (i.e., wherein each package implements a security model and includes an access mediation routine). The Final Office Action and previous Office Actions have failed to address this argument.

Also on page 8 of the Final Office Action, the Examiner asserts that "Hayman teaches incorporate and installation security software which inherently includes registering one or more packages of routines." The portion of *Hayman* that refer to the incorporation and installation of security software describe a Session Monitor. The "Session Monitor has been designed to be extensible, in the sense that the owner of the security system can incorporate their own software to change access mode of a user or administrator" (col. 8, line 66 – col. 9, line 2). Thus, the Examiner equates the Session Monitor with a package of routines.

The Session Monitor, however, "controls the manner in which a user or administrator initially **gains access to the system**, and the manner in which a user or administrator changes from their current mode of access to a different mode (for example, from user to administrator)" (col. 8, lines 55-60; emphasis added), whereas Claim 6 requires that a policy of a package is associated with a table within the database system. **There is no teaching or suggestion in *Hayman* that the Session Monitor, or any component thereof, is associated with a table within a database system**.

On page 8 of the Final Office Action, the Examiner also cites two paragraphs of *Hayman* that describe a Reference Monitor for teaching the first and third steps of Claim 6. "The Reference Monitor is the entity that mediates all requests for access to an object by a

subject, and thus controls whether, and to what extent, the subject is granted access to the object" (col. 9, lines 56-59). However, the reference does not disclose that a Reference Monitor may be registered so that it can be customized and implemented by the user. Indeed, the Reference Monitor was described in a version of Data General's security system as being "tightly integrated with Data General's operating system" (col. 1, lines 26-28). This indicates that customization is not readily possible and that the **Reference Monitor is actually an embedded native software component of the security system, not a separate package that can be registered**. Again, this is all in contradiction to the elements of Claims 6 and 26.

Col. 9, line 61 to col. 10, line 4 of *Hayman* further states:

> The various subject-to-object access policies described above can be implemented by storing various policy data in an Information Security Policy Table database, which is maintained as part of the Reference Monitor.
>
> The Information Security Policy Table database contains policy modules which the Reference Monitor must invoke to check access. This table can be configured when the system software is first installed, to meet the specific security policy of the specific computer system. Further, the table can be altered when the security policy of the enterprise changes.

Perhaps the Examiner equates (a) the policy modules in the Information Security Policy Table database of *Hayman* with the recited access mediation routine of Claims 6 and 26 and (b) the policy data stored in the Information Security Policy Table database of *Hayman* with the recited first policy of Claims 6 and 26. However, *Hayman* fails to teach or suggest that a policy module and policy data (1) originate from the **same** package (2) that is **registered** with a database management system.

The Examiner also alleges that *Hayman* col. 5, lines 18-60 teaches "associating a first policy of a first model set in a first package with" an object. To be clear, instead of an object, Claim 6 states that the first policy is associated with "a first table within the database system". The Examiner equates the "labels" described in the above cited portion of *Hayman* with the

"first policy" of Claim 6. However, the "first policy" of Claim 6 is a policy of a package **that is registered with a database management system. No where does *Hayman* teach or suggest in the above cited portion that a "label" is registered with a database management system**.

Thus, because *Hayman*, alone or in combination with *Ayi*, does not teach, suggest, or render obvious Claims 6 and 26, it is respectfully submitted that Claims 6 and 26 are patentable over the combination of *Hayman* and *Ayi*.

2. Claims 7-20 and 27-40

Claims 7-20 and 27-40 are dependent claims that depend on an independent claim that is discussed above. Because each of Claims 7-20 and 27-40 includes the limitations of claims upon which they depend, the dependent claims are patentable for at least those reasons the claims upon which the dependent claims depend are patentable. In addition, the dependent claims introduce additional limitations that may independently render them patentable. For example,

a) Claim 8

Claim 8 depends on Claims 7, which depends on Claim 6, and additionally recites the "step of forming said each package further comprising including one or more administrative routines for defining a policy for the model set." In rejecting Claim 8, the Final Office Action, on page 9, cites col. 9, line 55 to col. 10, line 4 of *Hayman*. However, that cited portion of *Hayman* fails to teach or suggest how the recited "each package" is formed, much less that a package is formed in the manner recited in Claim 8. Furthermore, that cited portion fails to teach or suggest the recited administrative routines, which are included in a package and are for "defining the first policy."

In fact, the Examiner cites the same portion of *Hayman* as allegedly disclosing both the recited access mediation routine and the recited one or more administrative routines. However, the Examiner fails to make any distinction between the recited access mediation routine and the recited one or more administrative routines.

b) Claims 10 and 30

Claims 10 and 30, which depend on Claims 6 and 26, respectively, additionally recite "the step of invoking an administrative routine of the first package for defining the first policy." In rejecting Claim 10, the Final Office Action, on page 10, cites col. 5, lines 18-60 of *Hayman*. However, that cited portion merely teaches that (a) labels are applied to each object (e.g., database object) and each subject (e.g., user); (b) a label consists of a hierarchy component and a category set component; and (c) if the label of a subject "dominates" the label of an object, then that subject may access the object. Nothing in this cited portion may be equated to the recited "first package" of Claim 10. Thus, this cited portion fails to teach or suggest anything related to a routine of a package, much less a routine "for defining the first policy."

c) Claims 11 and 31

Claims 11 and 31, which depend on Claims 10 and 30, respectively, additionally recite that the "step of invoking the administrative routine of the first package further comprising providing to the administrative routine of the first package a plurality of parameters including a policy name for the first policy and a plurality of label names for labels of the first policy." In rejecting Claim 11, the Final Office Action, on page 10, cites col. 5, lines 18-60 and col. 6, lines 45-67 of *Hayman*. As discussed above, col. 5, lines 18-60 fail to teach or suggest anything related to a package (i.e., that implements a security model) that includes an administrative routine for defining a policy. It is appears that col. 6, lines 45-67 of *Hayman* was only cited

because it refers to the term "administrative." However, nothing in that cited portion can be equated to the recited administrative **routine**.

Col. 6, lines 45-67 describes problems of a basic MAC (Mandatory Access Control) policy (col. 6, lines 42-44). Specifically, col. 6, lines 45-67 discuss (a) the problem of a low-level user that is given a limited administrative role; and (b) the problem of an administrator run a program that contains malicious code. Lines 65-67 merely states that these two problems are solved "by dividing the totality of MAC hierarchies into a small number of distinct and non-overlapping regions." This cited portion fails to even suggest that a plurality of parameters are provided to an administrative routine, much less the specific parameters recited.

d) Claims 13 and 33

Claims 13 and 33, which depend on Claims 6 and 26, respectively, additionally recites:

> associating a second policy of a second model set in a second package with a second table within the database system; and
> invoking the access mediation routine in the second package for determining whether to allow operation on data in the second table based on the second policy.

In rejecting Claim 13, the Final Office Action, on page 11, cites paragraphs 6-8 of *Ayi*. Paragraphs 6-8 state that (a) rules are defined that establish a policy; (b) one or more labels are generated based on the policy; (c) a dataset can include a plurality of fields; and (d) the rules can be defined as expressions. However, these paragraphs of *Ayi*, like *Hayman*, lack any teaching or suggestion of the recited second package, which includes a policy **and** an access mediation routine for determining, based on that policy, whether to allow an operation on data in a table.

e) Claims 20 and 40

Claims 20 and 40, which indirectly depend on Claims 6 and 26, respectively,

additionally recite "the step of storing the set of allowed labels in a session cache for a communication session between the database management system and the user." The Examiner cites col. 8, lines 54-67 of *Hayman* and paragraphs 6-8 of *Ayi* as allegedly disclosing this feature of Claim 20. This is incorrect. Although the cited portion of *Hayman* refers to a "Session Monitor" (which is discussed previously), both *Hayman* and *Ayi* lack any mention of the term cache or anything equivalent. Therefore, *Hayman* and *Ayi*, both individually and in combination, fail to even suggest that the recited set of allowed labels are stored in a session cache.

C. CONCLUSION AND PRAYER FOR RELIEF

Based on the foregoing, it is respectfully submitted that the rejection of Claims 1-40 under 35 U.S.C. § 103(a) as being unpatentable over the cited art lacks the requisite factual and legal bases. Appellants therefore respectfully request that the Honorable Board reverse the rejection of Claims 1-40 under 35 U.S.C. § 103(a).

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

/DanielDLedesma#57181/

Daniel D. Ledesma
Reg. No. 57,181

Date: June 10, 2008

2055 Gateway Place, Suite 550
San Jose, CA 95110-1083
Telephone: (408) 414-1080 ext. 229
Facsimile: (408) 414-1076

VIII. CLAIMS APPENDIX

1. (Original) A method for managing access to data in a database subject to a plurality of label-based security policies, the method comprising the steps of:

receiving, within a database management system, a request for performing an operation set of one or more operations on data in a table of the database;

determining which policies, of the plurality of label-based policies, apply to the table based on a policy set of one or more policies associated with the table; and

for each operation in the operation set, determining whether to perform the operation on a row of the table based on a set of labels associated with the row, the set of labels corresponding to the policy set.

2. (Original) A method according to Claim 1, further comprising adding a policy column to the table for each policy in the policy set associated with the table

3. (Original) A method according to Claim 2, further comprising storing a label, of the set of labels associated with the row, in a corresponding policy column of the row.

4. (Original) A method according to Claim 2, said step of determining which policies apply further comprising the step of determining whether a column is a policy column.

5. (Original) A method according to Claim 1, wherein the policy set associated with the table includes two or more policies of the plurality of label-based policies.

6. (previously presented) A method for managing access to data in a database based on a database policy set of one or more label-based security policies, the method comprising the steps of:

registering, with a database management system, one or more packages of routines, wherein each package of said one or more packages implements a security model that supports a model set of one or more policies of the database policy set and said each package includes an access mediation routine;

associating a first policy of a first model set in a first package with a first table within the database system; and

invoking the access mediation routine in the first package for determining whether to allow operation on data in the first table based on the first policy.

7. (Previously Presented) A method according to Claim 6, further comprising the step of forming said each package of said one or more packages so that the access mediation routine conforms to a specified interface for enforcing a policy in the database management system.

8. (Previously Presented) A method according to Claim 7, said step of forming said each package further comprising including one or more administrative routines for defining a policy for the model set.

9. (Original) A method according to Claim 8, said step of including one or more administrative routines for defining a policy further comprising including one or more

administrative routines for defining a name for a particular policy; labels for the particular policy; descriptions for the labels; and properties for the labels.

10. (Original) A method according to Claim 6, further comprising the step of invoking an administrative routine of the first package for defining the first policy.

11. (Previously Presented) A method according to Claim 10, said step of invoking the administrative routine of the first package further comprising providing to the administrative routine of the first package a plurality of parameters including a policy name for the first policy and a plurality of label names for labels of the first policy.

12. (Original) A method according to Claim 6, further comprising, in response to attempts to operate on data in a row in the table, the step of determining that the first policy applies to the table.

13. (original) A method according to Claim 6, further comprising the steps of:

associating a second policy of a second model set in a second package with a second table within the database system; and

invoking the access mediation routine in the second package for determining whether to allow operation on data in the second table based on the second policy.

14. (Original) A method according to Claim 13, wherein the second model in the second package is the same as the first model in the first package.

15. (Original) A method according to Claim 13, wherein the second model in the second package is different from the first model in the first package.

16. (Original) A method according to Claim 13, wherein the second table is the same as the first table.

17. (Original) A method according to Claim 13, wherein the second table is different from the first table.

18. (Original) A method according to Claim 6, said step of invoking the access mediation routine in the first package further comprising providing data indicating the first policy to the access mediation routine.

19. (Previously Presented) A method according to Claim 6, wherein.

the method further comprises the step of determining a set of allowed labels for the first policy for a user of the database management system;

said step of invoking the access mediation routine is performed during said step of determining the set of allowed labels; and

the user is allowed to operate on the data according to the first policy if the data is associated with a label for the first policy and the label is included in the set of allowed labels for the first policy.

20. (Original) A method according to Claim 19, further comprising the step of storing the set of allowed labels in a session cache for a communication session between the database management system and the user.

21. (original) A computer-readable medium carrying one or more sequences of instructions for managing access to data in a database subject to a plurality of label-based security policies, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

receiving a request for performing an operation set of one or more operations on data in a table of the database;

determining which policies, of the plurality of label-based policies, apply to the table based on a policy set of one or more policies associated with the table; and

for each operation in the operation set, determining whether to perform the operation on a row of the table based on a set of labels associated with the row, the set of labels corresponding to the policy set.

22. (original) A computer-readable medium according to Claim 21, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform the step of adding a policy column to the table for each policy in the policy set associated with the table

23. (original) A computer-readable medium according to Claim 22, wherein execution of the one or more sequences of instructions further causes the one or more processors to

perform the step of storing a label, of the set of labels associated with the row, in a corresponding policy column of the row.

24. (original) A computer-readable medium according to Claim 22, said step of determining which policies apply further comprising the step of determining whether a column is a policy column.

25. (original) A computer-readable medium according to Claim 21, wherein the policy set associated with the table includes two or more policies of the plurality of label-based policies.

26. (previously presented) A computer-readable medium carrying one or more sequences of instructions for managing access to data in a database based on a database policy set of one or more label-based security policies, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

registering, with a database management system, one or more packages of routines, wherein each package of said one or more packages implements a security model that supports a model set of one or more policies of the database policy set and said each package includes an access mediation routine;

associating a first policy of a first model set in a first package with a first table within the database system; and

invoking the access mediation routine in the first package for determining whether to allow operation on data in the first table based on the first policy.

27. (original) A computer-readable medium according to Claim 26, wherein the access mediation routine conforms to a specified interface for enforcing a policy in the database management system.

28. (previously presented) A computer-readable medium according to Claim 27, wherein said each package of said one or more packages includes one or more administrative routines for defining a policy for the model set.

29. (original) A computer-readable medium according to Claim 28, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform the step of defining a name for a particular policy; labels for the particular policy; descriptions for the labels; and properties for the labels.

30. (original) A computer-readable medium according to Claim 26, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform the step of invoking an administrative routine of the first package for defining the first policy.

31. (previously presented) A computer-readable medium according to Claim 30, said step of invoking the administrative routine of the first package further comprising providing to the administrative routine of the first package a plurality of parameters including a policy name for the first policy and a plurality of label names for labels of the first policy.

32. (original) A computer-readable medium according to Claim 26, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform, in response to attempts to operate on data in a row in the table, the step of determining that the first policy applies to the table.

33. (original) A computer-readable medium according to Claim 26, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform the steps of:

associating a second policy of a second model set in a second package with a second table within the database system; and

invoking the access mediation routine in the second package for determining whether to allow operation on data in the second table based on the second policy.

34. (original) A computer-readable medium according to Claim 33, wherein the second model in the second package is the same as the first model in the first package.

35. (original) A computer-readable medium according to Claim 33, wherein the second model in the second package is different from the first model in the first package.

36. (original) A computer-readable medium according to Claim 33, wherein the second table is the same as the first table.

37. (original) A computer-readable medium according to Claim 33, wherein the second table is different from the first table.

38. (original) A computer-readable medium according to Claim 26, said step of invoking the access mediation routine in the first package further comprising providing data indicating the first policy to the access mediation routine.

39. (previously presented) A computer-readable medium according to Claim 26, wherein.

execution of the one or more sequences of instructions further causes the one or more processors to perform the step of determining a set of allowed labels for the first policy for a user of the database management system;

said step of invoking the access mediation routine is performed during said step of determining the set of allowed labels; and

the user is allowed to operate on the data according to the first policy if the data is associated with a label for the first policy and the label is included in the set of allowed labels for the first policy.

40. (original) A computer-readable medium according to Claim 39, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform the step of storing the set of allowed labels in a session cache for a communication session between the database management system and the user.

IX. EVIDENCE APPENDIX PAGE

None.

X. RELATED PROCEEDINGS APPENDIX PAGE

None.